Appl. No. 10/521,429
Amendment and Response dated May 6, 2008
Reply to Office Action mailed November 7, 2007

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1.   (Currently Amended) ~~In a wireless network comprising a server and server software including an intelligent software agent, a~~ A method of automatically providing a secure connection between a ~~the~~ wireless network and a user-operated device seeking access to the wireless network, the method comprising:

~~in response to an initial request for access to the wireless network by the device~~

(a) having an individual user make an initial request for access to the wireless network, the initial request being made from a user-operated device;

(b) having the wireless network receive the initial request for access from the user-operated device;

(c) [[(a)]] automatically installing the software agent on the user-operated device, wherein the software agent is not resident on the user-operated device prior to the initial request for access;

(d) [[(b)]] executing the software agent on the user-operated device to gather information from the user-operated ~~requesting~~ device, including device information and user authentication information;

(e) [[(c)]] transmitting the device identification and user authentication information to a network server ~~the~~ server; and

(f) [[(d)]] verifying both the device identification and the user authentication information; wherein when successfully verified, storing the identification and authentication information on an authorized access list, providing a unique encryption key to the device for storage thereon and granting the requesting device access to the wireless network; and when unsuccessfully verified, storing the identification and

Appl. No. 10/521,429
Amendment and Response dated May 6, 2008
Reply to Office Action mailed November 7, 2007

authentication information on an unauthorized access list and denying the device access
to the wireless network.

2.   Original) The method of claim 1 further comprising, in response to a subsequent
request for access to the wireless network by the device—

        (a) receiving the unique key corresponding to the device;

        (b) retrieving the identification and authentication information corresponding to
the unique key;

        (c) comparing the identification and authentication information with the
authorized and unauthorized lists; and

        (d) based on the comparison, one of granting and denying the device access to the
wireless network.

3.   (Original) The method of claim 1, wherein the step of denying access comprises
generating a notification message that an unauthorized device has attempted to access the
network.

4.   (Original) The method of claim 1, wherein the step of granting access comprises
providing access in accordance with existing network access rights of the user operating
the device.

5.   (Original) The method of claim 1, further comprising the step of collecting
information relevant for billing the user for services accessed through the network.

6.   (Original) The method of claim 1, further comprising the step of collecting
information relevant for bandwidth allocation over the network.

7.   (Original) The method of claim 1, further comprising the step of determining the
geographical location of the device.

8.   (Original) The method of claim 1, further comprising the step of automatically
installing application software on the device.

Appl. No. 10/521,429
Amendment and Response dated May 6, 2008
Reply to Office Action mailed November 7, 2007

9.   (Original) The method of claim 1, wherein the encryption key is a certificate.

10.   (Original) The method of claim 1, wherein the network comprises an isolated network segment and the initial connection between the device and the network is limited to the isolated network segment.

11.   (Original) The method of claim 1, wherein the step of granting access further comprises conformity to a security policy with respect to access from multiple devices.

12.   (Original) The method of claim 1, wherein the user is defined as a guest user and given a temporary encryption key with guest network access rights.